How Cisco IT Deploys Closed-Circuit TV Cameras over the Secure IP Network

Cisco migrates fiber traffic to IP network and network video recorders to data center.

Cisco uses video surveillance to help keep its work environment secure. Two years ago, Cisco used a combination of cameras and video cassette recorders (VCRs) to monitor building entrances and other high-security locations on its campuses. Managing the VCRs, coaxial cabling, and tapes was labor intensive and prone to human error. Looking for a better solution, Cisco implemented closed-circuit TV (CCTV) over IP for surveillance. The system uses digital video and uses IP to carry the video signal across the network to digital video recorders in a centrally managed data center. Since making the change, Cisco has improved security, enhanced building access control, and significantly reduced security costs.

Cisco evaluated nine video-management software technologies before choosing a digital video system that runs on network video recorders (NVRs). Compatibility between the standards-based NVRs and existing security systems influenced Cisco's selection. The new NVR solution integrates well with the current Cisco building intrusion-detection system, smoke and fire alarm software, access-control badge readers, and visitor-management database.

The new system provided instant and tangible benefits. Network integration improved protection against network viruses and worms. Cisco reduced the time required to investigate security incidents, mitigated risk by expediting maintenance and repair, and centralized security analysis and investigation. Cisco lowered storage requirements by 60 percent—a US$500,000 savings—and reduced the number of servers by 40 percent—another $200,000 savings. In addition, the new system reduced maintenance costs by 20 percent and false alarms by 90 percent.

Cost savings are only part of the equation. Cisco plans to further enhance the system with video-analysis engines that monitor surveillance videos for violations of business rules. For example, the system would look for violations such as unattended packages or an individual standing in the same place for more than a specific amount of time.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.